WM9C3-15 Penetration Testing

21/22

Department
WMG

Level
Taught Postgraduate Level

Module leader
Harjinder Lallie

Credit value
15

Module duration
2 weeks

Assessment
Multiple

Study locations
University of Warwick main campus, Coventry Primary
Singapore Institute of Management, Singapore

Description

Introductory description

Increasing the robustness and resiliency of systems against threats and attacks is a key cyber security goal. Although, cyber security practitioners should be involved in system design early enough to design cyber-resiliency into the system, quite often, they are presented with legacy systems designed with little consideration to cyber-security. Notwithstanding, even well-designed systems are prone to cyber-attacks from both organised and ill-organised perpetrators.
Penetration testers must possess a good understanding of network protocols and design. This enables practitioners to gain a basic understanding of the root causes of network vulnerabilities and the associated remedial measures that can be taken, particularly where the root cause relates to network misconfiguration issues (both hardware and protocol related).

Module aims

This module aims to equip participants with the knowledge and practical experience of performing penetration/vulnerability testing and producing professional penetration testing reports for client organisations.
This module begins by providing an extensive understanding of networks including knowledge of network technology such as IPv4/6, and TCP/UDP. Participants proceed to understand the function and role that devices such as routers, switches and firewalls play in the security of a

network and the way that these devices should be configured to enable optimal security. Through the use of industry-standard simulation tools, the module equips participants with an in-depth practical applied knowledge of the importance of segregating differing trust domains via security devices such as routers, switches and stateful packet filtering firewalls as well as an understanding of how layered defence in depth aids the security of a network.
Having gained this practical knowledge, participants proceed to develop an in-depth knowledge of how to conduct a professional penetration test on a network. Participants are given an extensive knowledge of the phases of a penetration test which involve (for example) information gathering (reconnaissance), threat modelling, vulnerability analysis, exploitation. post-exploitation and reporting.
There is a fundamental emphasis on professionalism. Participants are made aware of the need to act professionally, in an ethical manner and are made aware of ‘responsible reporting’ programmes.
This module is partly taught by professional practitioners involved with professional penetration testing on a daily basis and also equipped with years of university academic experience*.

- reviewed on an annual basis.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Computer Networks

- Background. IP4/6 networks, addressing, routing, network architecture, trust domains; TCP/UDP, packet capture and analysis using tools such as Wireshark; Ingress and egress filtering via (stateful) packet firewalls.
- Network design. Enacting basic network design using tools such as packet tracer.
- Network security. Network security monitoring, passive, proactive, technical, non-technical, consequences; Operating system security, web security, embedded security, cloud and virtualisation security, security as a service
  Penetration testing
- Information gathering methods, techniques and tools. Footprinting, reconnaissance, network port scanning.
- Vulnerability exploitation. Gaining and maintaining access, covering tracks, enumeration techniques and vulnerability assessment, static and dynamic analysis of malware, social engineering, SQL injection, and zero-day exploits, session hijacking, denial-of-Service, password cracking, firewalking techniques, evading intrusion detection systems and firewalls, hacking web applications and SQL injection attacks.
- Penetration testing. Professionalism, ethics and responsible reporting; penetrations testing methodologies, standards and plans.

Learning outcomes

By the end of the module, students should be able to:

- Appraise the security posture of a network by analysing the network configuration using

appropriate tools where necessary.
- Critically evaluate the configuration of network security devices to achieve a desired security posture recommending adjustments where appropriate.
- Demonstrate a comprehensive understanding of vulnerability exploitation techniques.
- Assess the results of system security tests and recommend appropriate mitigation strategies – which may include possible design and configuration changes.

Indicative reading list

Andrew, S., 2011. Tanenbaum, and J. Wetherall. Computer Networks, 5th Edition, Morgan Kaufmann
Baloch, R., 2017. Ethical hacking and penetration testing guide. CRC Press.

Research element

There is a strong emphasis on the development, growth and enhancement of individual research skills so as to provide participants with the high level research knowledge, skills and competencies needed to undertake an independent, original piece of research. The module content draws upon and highlights research within the domain and the module assessment requires participants to perform further research before preparing a response to the assessment task.

Interdisciplinary

Although the module is largely dedicated towards the development of discipline-specific technical, professional and analytical skills, there is a small emphasis on the interdisciplinary nature of the subject.

International

The module is designed in such a way that it can be taught anywhere in the world. Learning materials and examples will be drawn from a range of disciplines, cultures and countries covering the whole range of subjects and disciplines taught in WMG. One of the key issues relating to internationalisation in this module is the way that penetration testing is managed in multiple jurisdictions. The approach to gaining consent varies from country to country and this is emphasised throughout the module.

Subject specific skills

Participants will develop an advanced applied understanding of system defence and offence principles, strategies, techniques and concepts through lectures, in-class discussion and case studies outlining a number of real-world practical issues and scenarios. Participants will develop hands-on experience of managing a penetration testing project from the beginning (elucidating requirements) through the development of a professional report aimed at senior management.

Transferable skills

A penetration test is essentially a project which must be managed effectively from the start (elucidating requirements) to completion (the generation of a report). This module therefore develops transferable skills such as project management, time and resource management, and report writing.
Typically, holders of the qualification will be able to:

- communicate conclusions clearly and effectively to specialist and non-specialist audiences
- apply critical thinking to interpreting and solving problems
- apply appropriate technical skills in new and challenging scenarios
- apply self-direction and originality in tackling and solving problems, and act autonomously in planning and implementing tasks at a professional or equivalent level
- organise and manage critical resources such as time, budget and finance

Study

Study time

Type	Required
Lectures	13 sessions of 1 hour (9%)
Tutorials	27 sessions of 1 hour (18%)
Online learning (independent)	30 sessions of 1 hour (20%)
Assessment	80 hours (53%)
Total	150 hours

Private study description

No private study requirements defined for this module.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Penetration test of a corporate network	80%	76 hours	Yes (extension)

	Weighting	Study time	Eligible for self-certification

Participants will be provided with a network specification in the form of a packet tracer network and a virtualised environment comprising of multiple servers. Participants will be required to plan, prepare, execute and report on a penetration test. The report is aimed at stakeholders with varied technical abilities from managers who have strong technical abilities to senior management interested only in an executive summary.

In module test testing the ability to	20%	4 hours	No

Participants are tested on their understanding of network configuration. Participants will be provided with a network in the form of a packet tracer environment which contains multiple faults. They will undertake a sequence of tests on the network and then determine problems with the configuration - making recommendations and changes as appropriate.

Assessment group R

	Weighting	Study time	Eligible for self-certification
Penetration test of a corporate network	100%		Yes (extension)

Participants will be provided with a network specification in the form of a packet tracer network and a virtualised environment comprising of multiple servers. These will be different to that provided in the first sitting. Participants will be required to plan, prepare, execute and report on a penetration test. The report is aimed at stakeholders with varied technical abilities from managers who have strong technical abilities to senior management interested only in an executive summary.

Feedback on assessment

Feedback will be provided as annotated commentary within the submitted work. High level feedback will be provided on a standard WMG feedback sheet. Students will have an opportunity to get further feedback and support directly from the module tutor.

Availability

Courses

This module is Core for:

- Cyber Security Management (New Degree)